

Cyclic Codes from Cyclotomic Sequences of Order Four

Cunsheng Ding

Abstract

Cyclic codes are an interesting subclass of linear codes and have been used in consumer electronics, data transmission technologies, broadcast systems, and computer applications due to their efficient encoding and decoding algorithms. In this paper, three cyclotomic sequences of order four are employed to construct a number of classes of cyclic codes over $\text{GF}(q)$ with prime length. Under certain conditions lower bounds on the minimum weight are developed. Some of the codes obtained are optimal or almost optimal. In general, the cyclic codes constructed in this paper are very good. Some of the cyclic codes obtained in this paper are closely related to almost difference sets and difference sets. As a byproduct, the p -rank of these (almost) difference sets are computed.

Index Terms

Almost difference sets, cyclic codes, cyclotomy, difference sets, sequences

I. INTRODUCTION

Let q be a power of a prime p . A linear $[n, k, d]$ code over $\text{GF}(q)$ is a k -dimensional subspace of $\text{GF}(q)^n$ with minimum (Hamming) nonzero weight d .

A linear $[n, k]$ code \mathcal{C} over the finite field $\text{GF}(q)$ is called *cyclic* if $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$. Let $\gcd(n, q) = 1$. By identifying any vector $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(q)^n$ with

$$c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} \in \text{GF}(q)[x]/(x^n - 1),$$

any code \mathcal{C} of length n over $\text{GF}(q)$ corresponds to a subset of $\text{GF}(q)[x]/(x^n - 1)$. The linear code \mathcal{C} is cyclic if and only if the corresponding subset in $\text{GF}(q)[x]/(x^n - 1)$ is an ideal of the ring $\text{GF}(q)[x]/(x^n - 1)$.

Note that every ideal of $\text{GF}(q)[x]/(x^n - 1)$ is principal. Let $\mathcal{C} = (g(x))$ be a cyclic code. Then $g(x)$ is called the *generator polynomial* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check polynomial* of \mathcal{C} .

A vector $(c_0, c_1, \dots, c_{n-1}) \in \text{GF}(q)^n$ is said to be *even-like* if $\sum_{i=0}^{n-1} c_i = 0$, and is *odd-like* otherwise. The minimum weight of the even-like codewords, respectively the odd-like codewords of a code is the minimum even-like weight, denoted by d_{even} , respectively the minimum odd-like weight of the code, denoted by d_{odd} .

The error correcting capability of cyclic codes may not be as good as some other linear codes in general. However, cyclic codes have wide applications in storage and communication systems because they have efficient encoding and decoding algorithms [9], [17], [25].

Cyclic codes have been studied for decades and a lot of progress has been made (see for example, [5], [8], [16], [19], [22]). The total number of cyclic codes over $\text{GF}(q)$ and their constructions are closely related to cyclotomic cosets modulo n , and thus many areas of number theory. An important problem in coding theory is to find simple ways to construct good cyclic codes.

In this paper, we construct cyclic codes over $\text{GF}(q)$ with length n and generator polynomial

$$\frac{x^n - 1}{\gcd(\Lambda(x), x^n - 1)} \quad (1)$$

where

$$\Lambda(x) = \sum_{i=0}^{n-1} \lambda_i x^i \in \text{GF}(q)[x]$$

and $\lambda^\infty = (\lambda_i)_{i=0}^\infty$ is a sequence of period n over $\text{GF}(q)$. Throughout this paper, we call the cyclic code \mathcal{C}_λ with the generator polynomial of (1) the *code defined by the sequence* λ^∞ , and the sequence λ^∞ the *defining sequence* of the cyclic code \mathcal{C}_λ . By employing three cyclotomic sequences λ^∞ over $\text{GF}(q)$, we will construct several classes of cyclic codes over $\text{GF}(q)$ with prime length. The cyclic codes presented in this paper are very good in general. Some of them are optimal or almost optimal. As a byproduct, the p -rank of some almost difference sets and difference sets are computed.

II. PRELIMINARIES

In this section, we present basic notations and results of combinatorial designs, cyclotomy, sequences, and cyclic codes that will be employed in subsequent sections.

A. Difference sets and almost difference sets

Let $(A, +)$ be an Abelian group of order n . Let C be a k -subset of A . The set C is an (n, k, λ) *difference set* of A if $d_C(w) = \lambda$ for every nonzero element of A , where $d_C(w)$ is the *difference function* defined by

$$d_C(w) = |C \cap (C + w)|,$$

here and hereafter $C + w := \{c + w : c \in C\}$. Detailed information on difference sets can be found in [4].

Let $(A, +)$ be an Abelian group of order n . A k -subset C of A is an (n, k, λ, t) *almost difference set* of A if $d_C(w)$ takes on λ altogether t times and $\lambda + 1$ altogether $n - 1 - t$ times when w ranges over all the nonzero elements of A . The reader is referred to [1] for information on almost difference sets.

Difference sets and almost difference sets are closely related to sequences with only a few autocorrelation values, and are related to some of the codes constructed in this paper.

B. The linear span and minimal polynomial of periodic sequences

Let $\lambda^n = \lambda_0 \lambda_1 \cdots \lambda_{n-1}$ be a sequence over $\text{GF}(q)$. The *linear span* (also called *linear complexity*) of λ^n is defined to be the smallest positive integer ℓ such that there are constants $c_0 = 1, c_1, \dots, c_\ell \in \text{GF}(q)$ satisfying

$$-c_0 \lambda_i = c_1 \lambda_{i-1} + c_2 \lambda_{i-2} + \cdots + c_\ell \lambda_{i-\ell} \text{ for all } \ell \leq i < n.$$

In engineering terms, such a polynomial $c(x) = c_0 + c_1 x + \cdots + c_\ell x^\ell$ is called the *feedback polynomial* of a shortest linear feedback shift register (LFSR) that generates λ^n . Such an integer always exists for finite sequences λ^n . When n is ∞ , a sequence λ^∞ is called a semi-infinite sequence. If there is no such an integer for a semi-infinite sequence λ^∞ , its linear span is defined to be ∞ . The linear span of the zero sequence is defined to be zero. For ultimately periodic semi-infinite sequences such an ℓ always exists.

Let λ^∞ be a sequence of period n over $\text{GF}(q)$. Any feedback polynomial of λ^∞ is called an *characteristic polynomial*. The characteristic polynomial with the smallest degree is called the *minimal polynomial* of the periodic sequence λ^∞ . Since we require that the constant term of any characteristic polynomial be 1, the minimal polynomial of any periodic sequence λ^∞ must be unique. In addition, any characteristic polynomial must be a multiple of the minimal polynomial.

For periodic sequences, there are a few ways to determine their linear span and minimal polynomials. One of them is given in the following lemma [21].

Lemma 2.1: Let λ^∞ be a sequence of period n over $\text{GF}(q)$. Define

$$\Lambda^n(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1} x^{n-1} \in \text{GF}(q)[x].$$

Then the minimal polynomial m_λ of λ^∞ is given by

$$\frac{x^n - 1}{\gcd(x^n - 1, \Lambda^n(x))}; \quad (2)$$

and the linear span \mathbb{L}_λ of λ^∞ is given by

$$n - \deg(\gcd(x^n - 1, \Lambda^n(x))). \quad (3)$$

C. Group characters and Gaussian sums

Let q be a power of a prime p . Let $\text{Tr}_{q/p}$ denote the trace function from $\text{GF}(q)$ to $\text{GF}(p)$. An *additive character* of $\text{GF}(q)$ is a nonzero function χ from $\text{GF}(q)$ to the set of complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \text{GF}(q)^2$. For each $b \in \text{GF}(q)$, the function

$$\chi_b(c) = e^{2\pi\sqrt{-1}\text{Tr}_{q/p}(bc)/p} \quad \text{for all } c \in \text{GF}(q) \quad (4)$$

defines an additive character of $\text{GF}(q)$. When $b = 0$, $\chi_0(c) = 1$ for all $c \in \text{GF}(q)$, and is called the *trivial additive character* of $\text{GF}(q)$. The character χ_1 in (4) is called the *canonical additive character* of $\text{GF}(q)$.

A *multiplicative character* of $\text{GF}(q)$ is a nonzero function ψ from $\text{GF}(q)^*$ to the set of complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for all pairs $(x, y) \in \text{GF}(q)^* \times \text{GF}(q)^*$. Let g be a fixed primitive element of $\text{GF}(q)$. For each $j = 0, 1, \dots, q-2$, the function ψ_j with

$$\psi_j(g^k) = e^{2\pi\sqrt{-1}jk/(q-1)} \quad \text{for } k = 0, 1, \dots, q-2 \quad (5)$$

defines a multiplicative character of $\text{GF}(q)$ with order k . When $j = 0$, $\psi_0(c) = 1$ for all $c \in \text{GF}(q)^*$, and is called the *trivial multiplicative character* of $\text{GF}(q)$.

Let ψ be a multiplicative character with order k where $k|(q-1)$ and χ an additive character of $\text{GF}(q)$. Then the *Gaussian sum* $G(\psi, \chi)$ of order k is defined by

$$G(\psi, \chi) = \sum_{c \in \text{GF}(q)^*} \psi(c)\chi(c).$$

Since $G(\psi, \chi_b) = \bar{\psi}(b)G(\psi, \chi_1)$, we just consider $G(\psi, \chi_1)$, briefly denoted as $G(\psi)$, in the sequel. If $\psi \neq \psi_0$, then

$$|G(\psi)| = q^{1/2}. \quad (6)$$

D. Cyclotomy

Let $r-1 = nN$ for two positive integers $n > 1$ and $N > 1$, and let α be a fixed primitive element of $\text{GF}(r)$. Define $C_i^{(N,r)} = \alpha^i \langle \alpha^N \rangle$ for $i = 0, 1, \dots, N-1$, where $\langle \alpha^N \rangle$ denotes the subgroup of $\text{GF}(r)^*$ generated by α^N . The cosets $C_i^{(N,r)}$ are called the *cyclotomic classes* of order N in $\text{GF}(r)$. The *cyclotomic numbers* of order N are defined by

$$(i, j)_N = \left| (C_i^{(N,r)} + 1) \cap C_j^{(N,r)} \right|$$

for all $0 \leq i \leq N-1$ and $0 \leq j \leq N-1$.

The following lemma is proved in [26] and will be useful in the sequel.

Lemma 2.2: If $r \equiv 1 \pmod{4}$, we have

$$(0, 0)_2 = \frac{r-5}{4}, \quad (0, 1)_2 = (1, 0)_2 = (1, 1)_2 = \frac{r-1}{4}.$$

If $r \equiv 3 \pmod{4}$, we have

$$(0, 1)_2 = \frac{r+1}{4}, \quad (0, 0)_2 = (1, 0)_2 = (1, 1)_2 = \frac{r-3}{4}.$$

E. Gaussian periods

The *Gaussian periods* are defined by

$$\eta_i^{(N,r)} = \sum_{x \in C_i^{(N,r)}} \chi(x), \quad i = 0, 1, \dots, N-1,$$

where χ is the canonical additive character of $\text{GF}(r)$.

Gaussian periods are closely related to Gaussian sums. By the discrete Fourier transform, it is known that

$$\begin{aligned} \eta_i^{(N,r)} &= \frac{1}{N} \sum_{j=0}^{N-1} \zeta_N^{-ij} G(\psi^j) \\ &= \frac{1}{N} \left[-1 + \sum_{j=1}^{N-1} \zeta_N^{-ij} G(\psi^j) \right] \end{aligned} \quad (7)$$

where $\zeta_N = e^{2\pi\sqrt{-1}/N}$ and ψ is a primitive multiplicative character of order N over $\text{GF}(r)^*$.

The values of the Gaussian periods are known in a few cases, but are in general very hard to compute. The following is proved in [15]

Theorem 2.3: For all i with $0 \leq i \leq N-1$, we have

$$\left| \eta_i^{(N,r)} + \frac{1}{N} \right| \leq \left\lfloor \frac{(N-1)\sqrt{r}}{N} \right\rfloor.$$

F. Bounds on the weights in irreducible cyclic codes

Let $\gcd(n, q) = 1$ and let $k := \text{ord}_n(q)$ denote the order of q modulo n . Define $r = q^k$. Let $N > 1$ be an integer dividing $r-1$, and put $n = (r-1)/N$. Let α be a primitive element of $\text{GF}(r)$ and define $\theta = \alpha^N$. The set

$$\mathcal{C}(r, N) = \left\{ (\text{Tr}_{r/q}(a\theta^i))_{i=0}^{n-1} : a \in \text{GF}(r) \right\} \quad (8)$$

is called an *irreducible cyclic* $[n, k]$ code over $\text{GF}(q)$, where $\text{Tr}_{r/q}$ is the trace function from $\text{GF}(r)$ onto $\text{GF}(q)$.

Using Delsarte's Theorem [10], one can prove that the code $\mathcal{C}(r, N)$ is the cyclic code with check polynomial $m_{\theta^{-1}}(x)$, which is the minimal polynomial of θ^{-1} over $\text{GF}(q)$ and is irreducible over $\text{GF}(q)$ (see also [21, Theorem 8.24]).

The determination of the weight distribution of irreducible cyclic codes is equivalent to that of the values of the Gaussian periods. Hence, the weight distribution of the irreducible cyclic codes is known for a few cases [15], but open in general.

The following is proved in [15] and will be useful in this paper.

Theorem 2.4: Let N be a positive divisor of $r-1$ and define $N_1 = \gcd((r-1)/(q-1), N)$. Let k be the multiplicative order of q modulo n . Then the set $\mathcal{C}(r, N)$ in (8) is a $[(q^m-1)/N, k]$ cyclic code over $\text{GF}(q)$ in which the weight w of every nonzero codeword satisfies that

$$\left\lceil \frac{r - \lfloor (N_1 - 1)\sqrt{r} \rfloor}{qN} \right\rceil \leq \frac{w}{q-1} \leq \left\lfloor \frac{r + \lfloor (N_1 - 1)\sqrt{r} \rfloor}{qN} \right\rfloor.$$

G. Lower bound on the minimum weight of a class of cyclic codes

Let $\gcd(n, q) = 1$ and let $k := \text{ord}_n(q)$ denote the order of q modulo n . Define $r = q^k$. Let $N > 1$ be an integer dividing $r - 1$, and put $n = (r - 1)/N$. Let α be a primitive element of $\text{GF}(r)$ and define $\theta = \alpha^N$. The set

$$\bar{\mathcal{C}}(r, N) = \left\{ \left(\text{Tr}_{r/q}(a\theta^i + b) \right)_{i=0}^{n-1} : a, b \in \text{GF}(r) \right\} \quad (9)$$

is a cyclic $[n, k + 1]$ code over $\text{GF}(q)$, where $\text{Tr}_{r/q}$ is the trace function from $\text{GF}(r)$ onto $\text{GF}(q)$.

Using Delsarte's Theorem [10], one can prove that the code $\bar{\mathcal{C}}(r, N)$ is the cyclic code with check polynomial $(x-1)m_{\theta^{-1}}(x)$, where $m_{\theta^{-1}}(x)$ is the minimal polynomial of θ^{-1} over $\text{GF}(q)$ and is irreducible over $\text{GF}(q)$.

Theorem 2.5: Let N be a positive divisor of $r - 1$ and define $N_1 = \gcd((r - 1)/(q - 1), N)$. Let k be the multiplicative order of q modulo n . Then the set $\bar{\mathcal{C}}(r, N)$ in (9) is a $[(q^m - 1)/N, k + 1, d]$ cyclic code over $\text{GF}(q)$, where

$$d \geq \min \left\{ (q - 1) \left\lceil \frac{r - \lfloor (N_1 - 1)\sqrt{r} \rfloor}{qN} \right\rceil, \frac{(q-1)(r-1)-1}{qN} - \frac{q-1}{q} \left\lfloor \frac{(N-1)\sqrt{r}}{N} \right\rfloor \right\}.$$

Proof: Let $\zeta_p = e^{2\pi\sqrt{-1}/p}$, and $\chi(x) = \zeta_p^{\text{Tr}_{r/p}(x)}$, where $\text{Tr}_{r/p}$ is the trace function from $\text{GF}(r)$ to $\text{GF}(p)$. Then χ is an additive character of $\text{GF}(r)$.

Let $b \in \text{GF}(r)$. We have

$$\begin{aligned} \sum_{y \in \text{GF}(q)} \chi(-by) &= \sum_{y \in \text{GF}(q)} \zeta_p^{\text{Tr}_{q/p}(\text{Tr}_{r/q}(-by))} \\ &= \sum_{y \in \text{GF}(q)} \zeta_p^{\text{Tr}_{q/p}(y \text{Tr}_{r/q}(-b))} \\ &= \begin{cases} 0 & \text{if } \text{Tr}_{r/q}(b) \neq 0 \\ q & \text{if } \text{Tr}_{r/q}(b) = 0. \end{cases} \end{aligned} \quad (10)$$

Note that the code $\bar{\mathcal{C}}(r, N)$ of (9) contains the code $\mathcal{C}(r, N)$ of (8) as a subcode. Define

$$\mathbf{c}_{(a,b)} = (\text{Tr}_{r/q}(a + b), \text{Tr}_{r/q}(a\theta + b), \dots, \text{Tr}_{r/q}(a\theta^{n-1} + b))$$

where $a, b \in \text{GF}(r)$.

If $\text{Tr}_{r/q}(b) = 0$, $\mathbf{c}_{(a,b)}$ is a codeword of the code $\mathcal{C}(r, N)$ of (8) and the Hamming weight of this codeword satisfies the bounds of Theorem 2.4. If $a = 0$ and $\text{Tr}_{r/q}(b) \neq 0$, the Hamming weight of $\mathbf{c}_{(a,b)}$ is equal to n .

We now consider the weight of $\mathbf{c}_{(a,b)}$ for the case that $a \neq 0$ and $\text{Tr}_{r/q}(b) \neq 0$. Let $Z(r, a, b)$ denote the number of solutions $x \in \text{GF}(r)$ of the equation $\text{Tr}_{r/q}(ax^N - b) = 0$. It then follows from (10) that

$$\begin{aligned} Z(r, a, b) &= \frac{1}{q} \sum_{y \in \text{GF}(q)} \sum_{x \in \text{GF}(r)} \zeta_p^{\text{Tr}_{q/p}(y \text{Tr}_{r/q}(ax^N - b))} \\ &= \frac{1}{q} \sum_{y \in \text{GF}(q)} \sum_{x \in \text{GF}(r)} \chi(y(ax^N - b)) \\ &= \frac{1}{q} \left[r - 1 + \sum_{y \in \text{GF}(q)^*} \sum_{x \in \text{GF}(r)^*} \chi(yax^N - b) \right] \\ &= \frac{1}{q} \left[r - 1 + N \sum_{y \in \text{GF}(q)^*} \sum_{x \in C_0^{(N,r)}} \chi(y(ax - b)) \right] \end{aligned} \quad (11)$$

Then the Hamming weight w of the codeword $\mathbf{c}_{(a,b)}$ is then given by

$$qNw = (q-1)(r-1) - N \sum_{y \in \text{GF}(q)^*} \sum_{x \in C_0^{(N,r)}} \chi(y(ax-b)). \quad (12)$$

It then follows that

$$w - \frac{(q-1)(r-1) - 1}{qN} = - \frac{\sum_{y \in \text{GF}(q)^*} \chi(-by) \left(\sum_{x \in C_0^{(N,r)}} \chi(ayx) + \frac{1}{N} \right)}{q}.$$

By Theorem 2.3, we have then

$$\left| w - \frac{(q-1)(r-1) - 1}{qN} \right| \leq \frac{q-1}{q} \left\lfloor \frac{(N-1)\sqrt{r}}{N} \right\rfloor.$$

Whence,

$$w \geq \frac{(q-1)(r-1) - 1}{qN} - \frac{q-1}{q} \left\lfloor \frac{(N-1)\sqrt{r}}{N} \right\rfloor. \quad (13)$$

Combining the lower bound of (13) and that of Theorem 2.4 proves the conclusions of this theorem. ■

III. CYCLIC CODES FROM CYCLOTOMIC SEQUENCES OF ORDER FOUR

A. Basic notations and results

Throughout this section, let n be an odd prime such that $n \equiv 1 \pmod{4}$. It is well known that n can be expressed as $n = u^2 + 4v^2$, where u is an integer with $u \equiv 1 \pmod{4}$ and the sign of v is undetermined. As usual, $q = p^m$ for a prime p and satisfies $\gcd(n, q) = 1$. Let $\text{ord}_n(q)$ denote the multiplicative order of q modulo n . Let η be an n th primitive root of unity over $\text{GF}(q^{\text{ord}_n(q)})$. Define for each i with $0 \leq i \leq 3$

$$\Omega_i^{(4,n)}(x) = \prod_{i \in C_i^{(4,n)}} (x - \eta^i),$$

where $C_i^{(4,n)}$ denotes the cyclotomic classes of order 4 in $\text{GF}(n)$. We have

$$x^n - 1 = \prod_{i=0}^3 \Omega_i^{(4,n)}(x).$$

It is straightforward to prove that $\Omega_i^{(4,n)}(x) \in \text{GF}(q)[x]$ if $q \in C_0^{(4,n)}$.

Note that the cyclotomic classes $C_0^{(4,n)}$ and $C_2^{(4,n)}$ do not depend on the choice of the generator of $\text{GF}(n)^*$ employed to define the cyclotomic classes. However, difference choices of the generator may lead to a swapping of $C_1^{(4,n)}$ and $C_3^{(4,n)}$. So we have the same conclusions for the four polynomials $\Omega_i^{(4,n)}(x)$.

By definition the cyclotomic classes of order 2 are given by

$$C_0^{(2,n)} = C_0^{(4,n)} \cup C_2^{(4,n)}, \quad C_1^{(2,n)} = C_1^{(4,n)} \cup C_3^{(4,n)}.$$

Define

$$\theta_0^{(2,n)} = \sum_{i \in C_0^{(2,n)}} \eta^i.$$

We now prove that

$$\theta_0^{(2,n)}(\theta_0^{(2,n)} + 1) = \frac{n-1}{4}. \quad (14)$$

In this case $-1 \in C_0^{(2,n)}$. By Lemma 2.2 we have

$$\begin{aligned} \left(\theta_0^{(2,n)}\right)^2 &= \left(\sum_{i \in C_0^{(2,n)}} \eta^i\right) \left(\sum_{j \in C_0^{(2,n)}} \eta^j\right) \\ &= \left(\sum_{i \in C_0^{(2,n)}} \eta^i\right) \left(\sum_{j \in C_0^{(2,n)}} \eta^{-j}\right) \\ &= \frac{n-1}{2} + \sum_{\substack{i,j \in C_0^{(2,n)} \\ i \neq j}} \eta^{i-j} \\ &= \frac{n-1}{4} - \theta_0^{(2,n)}. \end{aligned}$$

Hence, $\theta_0^{(2,n)} \in \{0, -1\}$ if and only if $(n-1)/4 \equiv 0 \pmod{p}$.

The following lemma will be useful in this section and can be proved with the Law of Biquadratic Reciprocity.

Lemma 3.1: We have the following conclusions:

- 2 is a biquadratic residue modulo $n \equiv 1 \pmod{4}$ if and only if $n = a^2 + 64b^2$ for some integers a and b .
- 3 is a biquadratic residue modulo $n \equiv 1 \pmod{4}$ if and only if $n = a^2 + 4b^2$ for some integers a and b and either
 - 1) $n \equiv 1 \pmod{8}$ and $b \equiv 0 \pmod{3}$, or
 - 2) $n \equiv 5 \pmod{8}$ and $a \equiv 0 \pmod{3}$.
- 5 is a biquadratic residue modulo $n = a^2 + b^2$, where b is even, if and only if $b \equiv 0 \pmod{5}$.

Lemma 3.2: Let $\text{ord}_n(q) = (n-1)/4$ and $q-1 < n$. Assume that $q \in C_0^{(4,n)}$. Then the cyclic code over $\text{GF}(q)$ with parity check polynomial $\Omega_i^{(4,n)}(x)$ has parameters $[n, (n-1)/4, d_i]$, where

$$d \geq (q-1) \left\lceil \frac{q^{\frac{n-1}{4}} - \left\lfloor (N_1 - 1) \sqrt{q^{\frac{n-1}{4}}} \right\rfloor}{qN} \right\rceil$$

and

$$N = \frac{q^{\frac{n-1}{4}} - 1}{n} \text{ and } N_1 = \frac{N}{q-1}.$$

Proof: Since $\text{ord}_n(q) = (n-1)/4$ and $q \in C_0^{(4,n)}$, the four polynomials $\Omega_i^{(4,n)}(x)$ are irreducible and over $\text{GF}(q)$. Hence the code with parity check polynomial $\Omega_i^{(4,n)}(x)$ is an irreducible cyclic code with dimension $(n-1)/4$.

Note that $q-1 < n$ and n is prime. We have then

$$\gcd\left(\frac{q^{\frac{n-1}{4}} - 1}{q-1}, N\right) = \frac{N}{q-1}.$$

The desired bounds on the nonzero weights follow from Theorem 2.4. ■

Example 3.3: Let $q = 3$ and $n = 13$. We have then the canonical factorization

$$x^{13} - 1 = (x + 2)(x^3 + 2x + 2)(x^3 + 2x^2 + 2) \times (x^3 + x^2 + x + 2)(x^3 + 2x^2 + 2x + 2).$$

The cyclic code with parity check polynomial $x^3 + 2x + 2$ has parameters $[13, 3, 9]$.

In this case $N = 2$ and $N_1 = 1$. The lower and upper bound in Lemma 3.2 are equal to 9.

In general, the bounds are tight if N_1 is small.

Lemma 3.4: Let $\text{ord}_n(q) = (n - 1)/4$ and $q - 1 < n$. Assume that $q \in C_0^{(4,n)}$. Then the cyclic code over $\text{GF}(q)$ with parity check polynomial $(x - 1)\Omega_i^{(4,n)}(x)$ has parameters $[n, (n + 3)/4, d_i]$, where

$$d_i \geq \frac{(q - 1)(q^{\frac{n-1}{4}} - 1) - 1}{qN} - \frac{q - 1}{q} \left\lfloor \frac{(N - 1)\sqrt{q^{\frac{n-1}{4}}}}{N} \right\rfloor$$

and

$$N = \frac{q^{\frac{n-1}{4}} - 1}{n}.$$

Proof: Since $\text{ord}_n(q) = (n - 1)/4$ and $q \in C_0^{(4,n)}$, the four polynomials $\Omega_i^{(4,n)}(x)$ are irreducible and over $\text{GF}(q)$. Hence the code with parity check polynomial $(x - 1)\Omega_i^{(4,n)}(x)$ has dimension $(n + 3)/4$, and is the same as the code of (9).

Note that $q - 1 < n$ and n is prime. We have then

$$\gcd\left(\frac{q^{\frac{n-1}{4}} - 1}{q - 1}, N\right) = \frac{N}{q - 1}.$$

The desired lower bound on the minimum weight follow from Theorem 2.5. ■

Example 3.5: Let $q = 3$ and $n = 13$. We have then the canonical factorization

$$x^{13} - 1 = (x + 2)(x^3 + 2x + 2)(x^3 + 2x^2 + 2) \times (x^3 + x^2 + x + 2)(x^3 + 2x^2 + 2x + 2).$$

The cyclic code with parity check polynomial $(x^3 + 2x + 2)(x - 1)$ has parameters $[13, 4, 7]$.

In this case $N = 2$ and $N_1 = 1$. The lower and upper bound in Lemma 3.2 are equal to 7.

In general, the lower bound is tight if N is small.

B. The first class of cyclic codes from cyclotomic sequences of order 4

Define

$$\lambda_i = \begin{cases} 1 & \text{if } i \bmod n \in C_0^{(4,n)} \cup C_1^{(4,n)} \\ 0 & \text{otherwise} \end{cases} \quad (15)$$

for all $i \geq 0$. This λ^∞ was defined as a binary sequence in [12] and was proved to have optimal autocorrelation under certain condition. Here in this section, we treat it as a sequence over $\text{GF}(q)$ for any prime power q , and employ it to construct cyclic codes.

We define

$$\begin{aligned} \Lambda(x) &= \sum_{i \in C_0^{(4,n)} \cup C_1^{(4,n)}} x^i \in \text{GF}(q)[x], \\ \Gamma(x) &= \sum_{i \in C_1^{(4,n)} \cup C_2^{(4,n)}} x^i \in \text{GF}(q)[x]. \end{aligned}$$

Both $\Lambda(x)$ and $\Gamma(x)$ depend on the choice of the generator of $\text{GF}(n)^*$ employed to define the cyclotomic classes of order 4.

Notice that

$$\left(\sum_{i \in C_0^{(4,n)}} + \sum_{i \in C_1^{(4,n)}} + \sum_{i \in C_2^{(4,n)}} + \sum_{i \in C_3^{(4,n)}} \right) \eta^i = -1.$$

We have then

$$\Lambda(\eta^i) = \begin{cases} \Lambda(\eta) & \text{if } i \in C_0^{(4,n)} \\ \Gamma(\eta) & \text{if } i \in C_1^{(4,n)} \\ -(\Lambda(\eta) + 1) & \text{if } i \in C_2^{(4,n)} \\ -(\Gamma(\eta) + 1) & \text{if } i \in C_3^{(4,n)}. \end{cases} \quad (16)$$

We have also that

$$\Lambda(\eta^0) = \Lambda(1) = \frac{n-1}{2} \pmod{p}. \quad (17)$$

Theorem 3.6: Let $\frac{n-1}{4} \equiv 0 \pmod{p}$, and let λ^∞ be the sequence of period n over $\text{GF}(q)$ defined in (15). As before, $n = u^2 + 4v^2$ with $u \equiv 1 \pmod{4}$.

1) $n \equiv 1 \pmod{8}$.

When $\frac{v}{2} \not\equiv 0 \pmod{p}$, we have $\mathbb{L}_\lambda = n - 1$ and

$$m_\lambda(x) = \frac{x^n - 1}{x - 1}.$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ above and parameters $[n, 1, n]$.

When $\frac{v}{2} \equiv 0 \pmod{p}$ and $q \in C_0^{(4,n)}$, we have $\mathbb{L}_\lambda = (n - 1)/2$ and

$$m_\lambda(x) = \begin{cases} \Omega_2^{(4,n)}(x)\Omega_3^{(4,n)}(x) & \text{if } \begin{cases} \Lambda(\eta) = 0 \\ \Gamma(\eta) = 0 \end{cases} \\ \Omega_1^{(4,n)}(x)\Omega_2^{(4,n)}(x) & \text{if } \begin{cases} \Lambda(\eta) = 0 \\ \Gamma(\eta) = -1 \end{cases} \\ \Omega_0^{(4,n)}(x)\Omega_3^{(4,n)}(x) & \text{if } \begin{cases} \Lambda(\eta) = -1 \\ \Gamma(\eta) = 0 \end{cases} \\ \Omega_0^{(4,n)}(x)\Omega_1^{(4,n)}(x) & \text{if } \begin{cases} \Lambda(\eta) = -1 \\ \Gamma(\eta) = -1 \end{cases} \end{cases}$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ above and parameters $[n, (n + 1)/2, d]$. In addition, the minimum odd-like weight $d_{\text{odd}} \geq \sqrt{n}$.

2) $n \equiv 5 \pmod{8}$.

When $\frac{u^2+3}{4} \not\equiv 0 \pmod{p}$, we have $\mathbb{L}_\lambda = n - 1$ and

$$m_\lambda(x) = \frac{x^n - 1}{x - 1}.$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ above and parameters $[n, 1, n]$.

When $\frac{u^2+3}{4} \equiv 0 \pmod{p}$ and $q \in C_0^{(4,n)}$, we have $\mathbb{L}_\lambda = 3(n-1)/4$ and

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_0^{(4,n)}(x)} & \text{if } \Lambda(\eta) = 0 \\ \frac{x^n-1}{(x-1)\Omega_2^{(4,n)}(x)} & \text{if } \Lambda(\eta) = -1 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)} & \text{if } \Gamma(\eta) = 0 \\ \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)} & \text{if } \Gamma(\eta) = -1. \end{cases}$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ above and parameters $[n, (n+3)/4, d]$. Furthermore, the minimum weight d has the lower bound of Lemma 3.4 if $\text{ord}_n(q) = (n-1)/4$.

Proof: To prove this theorem, we need information on cyclotomic numbers of order 4. When $n \equiv 5 \pmod{8}$ is odd, the relation between the 16 cyclotomic numbers of order 4 is given by the following Table I [26]:

$(h, k)_4$	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

TABLE I
THE RELATIONS OF THE CYCLOTOMIC NUMBERS OF ORDER 4, WHEN $n \equiv 5 \pmod{8}$.

Thus, there are five possible different cyclotomic numbers in this case; i.e.,

$$\begin{aligned} A &= \frac{n-7+2u}{16}, \\ B &= \frac{n+1+2u-8v}{16}, \\ C &= \frac{n+1-6u}{16}, \\ D &= \frac{n+1+2u+8v}{16}, \\ E &= \frac{n-3-2u}{16}. \end{aligned}$$

When $n \equiv 1 \pmod{8}$, the relation between the 16 cyclotomic numbers is given by the following Table II [26]:

$(h, k)_4$	0	1	2	3
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

TABLE II
THE RELATIONS OF THE CYCLOTOMIC NUMBERS OF ORDER 4, WHEN $n \equiv 1 \pmod{8}$.

Thus, there are five possible different cyclotomic numbers in this case; i.e.,

$$\begin{aligned} A &= \frac{n-11-6u}{16}, \\ B &= \frac{n-3+2u+8v}{16}, \\ C &= \frac{n-3+2u}{16}, \\ D &= \frac{n-3+2u-8v}{16}, \\ E &= \frac{n+1-2u}{16}. \end{aligned}$$

To determine the minimal polynomial $m_\lambda(x)$, we need to compute $\gcd(\Lambda(x), x^n - 1)$.

We first prove the conclusions for the case that $n \equiv 1 \pmod{8}$. In this case $-1 \in C_0^{(4,n)}$ and v must be even. Note that $\frac{n-1}{4} \equiv 0 \pmod{p}$. It then follows from the relations of the cyclotomic numbers and the cyclotomic numbers above that

$$\begin{aligned} &\Lambda(\eta)^2 \\ &= \sum_{i \in C_0^{(4,n)}, j \in C_0^{(4,n)}} \eta^{i-j} + \sum_{i \in C_0^{(4,n)}, j \in C_1^{(4,n)}} \eta^{i-j} + \\ &\quad \sum_{i \in C_1^{(4,n)}, j \in C_0^{(4,n)}} \eta^{i-j} + \sum_{i \in C_1^{(4,n)}, j \in C_1^{(4,n)}} \eta^{i-j} \\ &= ((0,0)_4 + (1,0)_4 + (0,1)_4 + (1,1)_4) \sum_{i \in C_0^{(4,n)}} \eta^i + \\ &\quad ((3,3)_4 + (0,3)_4 + (3,0)_4 + (0,0)_4) \sum_{i \in C_1^{(4,n)}} \eta^i + \\ &\quad ((2,2)_4 + (3,2)_4 + (2,3)_4 + (3,3)_4) \sum_{i \in C_2^{(4,n)}} \eta^i + \\ &\quad ((1,1)_4 + (2,1)_4 + (1,2)_4 + (2,2)_4) \sum_{i \in C_3^{(4,n)}} \eta^i + \\ &\quad \frac{n-1}{2} \\ &= (A+2B+D) \sum_{i \in C_0^{(4,n)}} \eta^i + (A+B+2D) \sum_{i \in C_1^{(4,n)}} \eta^i + \\ &\quad (B+C+2E) \sum_{i \in C_2^{(4,n)}} \eta^i + (C+D+2E) \sum_{i \in C_3^{(4,n)}} \eta^i \\ &\quad + \frac{n-1}{2} \\ &= \frac{n-5+2v}{4} \sum_{i \in C_0^{(4,n)}} \eta^i + \frac{n-5-2v}{4} \sum_{i \in C_1^{(4,n)}} \eta^i + \\ &\quad \frac{n-1+2v}{4} \sum_{i \in C_2^{(4,n)}} \eta^i + \frac{n-1-2v}{4} \sum_{i \in C_3^{(4,n)}} \eta^i \\ &\quad + \frac{n-1}{2} \end{aligned}$$

$$\begin{aligned}
&= -\Lambda(\eta) + \frac{n-1}{4} + \frac{v}{2} \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right) \\
&= -\Lambda(\eta) + \frac{v}{2} \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right)
\end{aligned}$$

Whence,

$$\Lambda(\eta)(\Lambda(\eta) + 1) = \frac{v}{2} \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right). \quad (18)$$

Note that $\frac{n-1}{4} \equiv 0 \pmod{p}$. By (14) we have $\sum_{i \in C_0^{(2,n)}} \eta^i \in \{0, -1\}$. It then follows that

$$2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \in \{1, -1\}. \quad (19)$$

Similarly, one can show that

$$\Gamma(\eta)(\Gamma(\eta) + 1) = -\frac{v}{2} \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right). \quad (20)$$

The desired conclusions on the linear span and the minimal polynomial of the sequence λ^∞ for Case 1 then follow from (16), (17), (18), (19), (20), and Lemma 2.1. The dimension and the generator polynomial of the code \mathcal{C}_λ follow from the conclusions on the linear span and the minimal polynomial of the sequence and the definition of the code \mathcal{C}_λ . In the first subcase, it is obvious that the minimum nonzero weight $d = n$. In the second subcase, the generator polynomial of the code shows that \mathcal{C}_λ is a duadic code. So we have the square-root bound on the minimum odd-like weight [19], [20], [24], [13], [14].

We now prove the conclusions for Case 2. Since $n \equiv 5 \pmod{8}$, $-1 \in C_2^{(4,n)}$. In this case v must be odd. Note that $\frac{n-1}{4} \equiv 0 \pmod{p}$. It then follows from the relations of the cyclotomic numbers and the cyclotomic numbers above that

$$\begin{aligned}
&\Lambda(\eta)^2 \\
&= \sum_{i \in C_0^{(4,n)}, j \in C_2^{(4,n)}} \eta^{i-j} + \sum_{i \in C_0^{(4,n)}, j \in C_3^{(4,n)}} \eta^{i-j} + \\
&\quad \sum_{i \in C_1^{(4,n)}, j \in C_2^{(4,n)}} \eta^{i-j} + \sum_{i \in C_1^{(4,n)}, j \in C_3^{(4,n)}} \eta^{i-j} \\
&= ((2, 0)_4 + (3, 0)_4 + (2, 1)_4 + (3, 1)_4) \sum_{i \in C_0^{(4,n)}} \eta^i + \\
&\quad ((1, 3)_4 + (2, 3)_4 + (1, 0)_4 + (2, 0)_4) \sum_{i \in C_1^{(4,n)}} \eta^i + \\
&\quad ((0, 2)_4 + (1, 2)_4 + (0, 3)_4 + (1, 3)_4) \sum_{i \in C_2^{(4,n)}} \eta^i + \\
&\quad ((3, 1)_4 + (0, 1)_4 + (3, 2)_4 + (0, 2)_4) \sum_{i \in C_3^{(4,n)}} \eta^i
\end{aligned}$$

$$\begin{aligned}
&= (A + D + 2E) \sum_{i \in C_0^{(4,n)}} \eta^i + \\
&\quad (A + B + 2E) \sum_{i \in C_1^{(4,n)}} \eta^i + \\
&\quad (B + C + 2D) \sum_{i \in C_2^{(4,n)}} \eta^i + \\
&\quad (C + D + 2B) \sum_{i \in C_3^{(4,n)}} \eta^i + \frac{n-1}{2} \\
&= -\Lambda(\eta) - \frac{n-1}{4} + \frac{v \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right) - 1}{2} \\
&= -\Lambda(\eta) + \frac{v \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right) - 1}{2}.
\end{aligned}$$

Whence,

$$\Lambda(\eta)(\Lambda(\eta) + 1) = \frac{v \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right) - 1}{2}. \quad (21)$$

Similarly, one can show that

$$\Gamma(\eta)(\Gamma(\eta) + 1) = -\frac{v \left(2 \sum_{i \in C_0^{(2,n)}} \eta^i + 1 \right) + 1}{2}. \quad (22)$$

Since $n \equiv 5 \pmod{8}$ and p divides $(n-1)/4$, p must be odd. Note that

$$\frac{n-1}{4} = \frac{u^2+3}{4} + (|v|-1)(|v|+1).$$

Hence, $\frac{u^2+3}{4} \equiv 0 \pmod{p}$ if and only if $(|v|-1)(|v|+1) \equiv 0 \pmod{p}$. However, $(|v|-1)(|v|+1) \equiv 0 \pmod{p}$ if and only if p divides one and only one of $|v|-1$ and $|v|+1$.

The desired conclusions on the linear span and the minimal polynomial of the sequence λ^∞ for Case 2 then follow from (16), (17), (21), (19), (22), and Lemma 2.1. The dimension and the generator polynomial of the code \mathcal{C}_λ follow from the conclusions on the linear span and the minimal polynomial of the sequence and the definition of the code \mathcal{C}_λ . In the first subcase, it is obvious that the minimum nonzero weight $d = n$. In the second subcase, the format of the generator polynomial of the code shows that the minimum weight d has the lower bound of Lemma 3.4 if $\text{ord}_n(q) = (n-1)/4$. \blacksquare

Example 3.7: Let $(p, m, n) = (2, 1, 73)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 4^2$. Hence $v/2 \pmod{p} = 0$. Then \mathcal{C}_λ is a $[73, 37, 12]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned}
&x^{36} + x^{35} + x^{34} + x^{32} + x^{31} + x^{29} + x^{28} + \\
&x^{27} + x^{25} + x^{23} + x^{18} + x^{13} + x^{11} + x^9 + \\
&x^8 + x^7 + x^5 + x^4 + x^2 + x + 1.
\end{aligned}$$

The best binary linear code known of length 73 and dimension 37 has minimum weight 14.

Example 3.8: Let $(p, m, n) = (2, 1, 89)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 4^2$. Hence $v/2 \pmod{p} = 0$. Then \mathcal{C}_λ is a $[89, 45, 15]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned}
&x^{44} + x^{43} + x^{42} + x^{41} + x^{40} + x^{35} + x^{34} + \\
&x^{33} + x^{31} + x^{26} + x^{24} + x^{23} + x^{22} + x^{21} + \\
&x^{20} + x^{18} + x^{13} + x^{11} + x^{10} + x^9 + x^4 + \\
&x^3 + x^2 + x + 1.
\end{aligned}$$

The best binary linear code known of length 89 and dimension 45 has minimum weight 17.

Example 3.9: Let $(p, m, n) = (3, 1, 13)$. Then $q = 3 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 1^2$. Hence $(u^2 + 3)/4 \bmod p = 0$. Then \mathcal{C}_λ is a $[13, 4, 7]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^9 + x^7 + x^6 + 2x^4 + x^2 + 2x + 2.$$

This code is optimal.

Example 3.10: Let $(p, m, n) = (7, 1, 29)$. Then $q = 7 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 1^2$. Hence $(u^2 + 3)/4 \bmod p = 0$. Then \mathcal{C}_λ is a $[29, 8, 15]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned} & x^{21} + 2x^{20} + 2x^{19} + 6x^{18} + x^{17} + 4x^{16} + 4x^{15} + \\ & 4x^{13} + 2x^{12} + 6x^{11} + 5x^{10} + x^9 + 2x^8 + 3x^7 + \\ & 3x^6 + x^5 + 4x^3 + 2x^2 + x + 6. \end{aligned}$$

This is the best cyclic code over $\text{GF}(q)$ with length 29 and dimension 8. The best linear code over $\text{GF}(q)$ with length 29 and dimension 8 has minimum weight 17.

Remark 3.11: It was proved in [12] that the sequence λ^∞ defined in (15) has optimal autocorrelation and the set $C_0^{(4,n)} \cup C_1^{(4,n)}$ is an $(n, (n-1)/2, (n-5)/4, (n-1)/2)$ almost difference set in $\text{GF}(n)$ when $v = \pm 1$. Examples 3.9 and 3.10 demonstrate that the cyclic codes defined by the almost difference sets have good parameters.

Open Problem 3.12: Determine the parameters of the code \mathcal{C}_λ defined by the sequence λ^∞ of (15) for the case that $\frac{n-1}{4} \not\equiv 0 \pmod{p}$.

C. The second class of cyclic codes from cyclotomic sequences of order 4

Unless otherwise stated, the symbols and notations of this section are the same as those in Section III-B. In this section, we always assume that $q \in C_0^{(4,n)}$. This ensures that the polynomials $\Omega_i^{(4,n)}(x)$ defined in Section III-A are over $\text{GF}(q)$. In this section, we also assume that $\frac{n-1}{4} \bmod p = 0$. Our task of this section is to construct more cyclic codes over $\text{GF}(q)$ using two cyclotomic sequences of order four.

The two sequences we will employ in this section are defined by

$$\lambda_i = \begin{cases} 1 & \text{if } i \bmod n \in C_1^{(4,n)} \cup C_2^{(4,n)} \cup C_3^{(4,n)} \\ 0 & \text{if } i \bmod n \in C_0^{(4,n)} \\ \rho & \text{if } i \bmod n = 0 \end{cases} \quad (23)$$

for all $i \geq 0$, where $\rho \in \{0, 1\}$. These two sequences λ^∞ are characterized by the cyclotomic class $C_0^{(4,n)}$, and are viewed as sequences over $\text{GF}(q)$ for any prime power q .

We define

$$\Lambda(x) = \rho + \sum_{i \in C_1^{(4,n)} \cup C_2^{(4,n)} \cup C_3^{(4,n)}} x^i \in \text{GF}(q)[x].$$

Let η be an n th primitive root of unity over $\text{GF}(q^{\text{ord}_n(q)})$. We define

$$\eta_i = \sum_{\ell \in C_i^{(4,n)}} \eta^\ell$$

for each $i \in \{0, 1, 2, 3\}$. Because of the assumption that $\frac{n-1}{4} \bmod p = 0$, by (14) we have

$$\eta_0 + \eta_2 = \sum_{i \in C_0^{(4,n)} \cup C_2^{(4,n)}} \eta^i = \sum_{i \in C_0^{(2,n)}} \eta^i \in \{0, -1\}. \quad (24)$$

The value $\eta_0 + \eta_2$ depends on the choice of η . Throughout this section, we fix an η such that $\eta_0 + \eta_2 = 0$. Notice that

$$\eta_0 + \eta_1 + \eta_2 + \eta_3 = -1.$$

We have then

$$\eta_1 + \eta_3 = -1.$$

It is easily seen that

$$\Lambda(\eta) = \rho - 1 - \sum_{i \in C_0^{(4,n)}} \eta^i$$

and

$$\Lambda(\eta^j) = \rho - 1 - \eta_i \quad (25)$$

if $j \in C_i^{(4,n)}$.

Due to the assumption that $\frac{n-1}{4} \bmod p = 0$,

$$\Lambda(\eta^0) = \Lambda(1) = \rho. \quad (26)$$

When $n \equiv 1 \pmod{8}$, the linear span and minimal polynomial of the sequence λ^∞ as well as the parameters of the code \mathcal{C}_λ are given in the following theorem.

Theorem 3.13: Let $\frac{n-1}{4} \equiv 0 \pmod{p}$ and $q \in C_0^{(4,n)}$, and let $n \equiv 1 \pmod{8}$. let λ^∞ be the sequence of period n over $\text{GF}(q)$ defined in (23). As before, $n = u^2 + 4v^2$ with $u \equiv 1 \pmod{4}$.

1) When $\frac{n+1-2u}{16} \equiv 0 \pmod{p}$ and $\frac{n-3+2u}{16} \equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)} & \text{if } \begin{cases} \eta_1 = 0 \\ \rho = 0 \end{cases} \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)} & \text{if } \begin{cases} \eta_1 = -1 \\ \rho = 0 \end{cases} \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \begin{cases} \eta_1 = 0 \\ \rho = 1 \end{cases} \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \begin{cases} \eta_1 = -1 \\ \rho = 1. \end{cases} \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+3}{4} & \text{if } \eta_1 = 0 \text{ and } \rho = 0 \\ n - \frac{n+3}{4} & \text{if } \eta_1 = -1 \text{ and } \rho = 0 \\ n - \frac{3n-3}{4} & \text{if } \eta_1 = 0 \text{ and } \rho = 1 \\ n - \frac{3n-3}{4} & \text{if } \eta_1 = -1 \text{ and } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_1 = 0$ and $\rho = 0$ or $\eta_1 = -1$ and $\rho = 0$, the minimum weight d of the code has the lower bound of Lemma 3.4, provided that $\text{ord}_n(q) = (n-1)/4$.

2) When $\frac{n+1-2u}{16} \equiv 0 \pmod{p}$ and $\frac{n-3+2u}{16} \not\equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{x-1} & \text{if } \rho = 0 \\ \frac{x^n-1}{\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - 1 & \text{if } \rho = 0 \\ n - \frac{n-1}{2} & \text{if } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$, where

$$\begin{cases} d = n & \text{if } \rho = 0 \\ d \geq \sqrt{n} & \text{if } \rho = 1. \end{cases}$$

- 3) When $\frac{n+1-2u}{16} \equiv 1 \pmod{p}$ and $\frac{n-3+2u}{16} \equiv 0 \pmod{p}$, we distinguish between the two subcases:
 p odd and $p = 2$.

If p is odd, we have

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_0 = 1, \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_0 = 1, \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x)} & \text{if } \eta_0 = -1, \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x)} & \text{if } \eta_0 = -1, \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 1 \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+1}{2} & \text{if } \eta_0 = 1, \eta_1 = 0, \rho = 0 \\ n - \frac{n+1}{2} & \text{if } \eta_0 = 1, \eta_1 = -1, \rho = 0 \\ n - \frac{n+1}{2} & \text{if } \eta_0 = -1, \eta_1 = 0, \rho = 0 \\ n - \frac{n+1}{2} & \text{if } \eta_0 = -1, \eta_1 = -1, \rho = 0 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = 0, \rho = 1 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = -1, \rho = 1. \end{cases}$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_1 = 0$ and $\rho = 1$ or $\eta_1 = -1$ and $\rho = 1$, the minimum weight d of the code has the lower bound of Lemma 3.2, provided that $\text{ord}_n(q) = (n-1)/4$. In the rest four cases, the code is a duadic code and the minimum odd-like weigh $d_{\text{odd}} \geq \sqrt{n}$.

If $p = 2$, we have

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 1 \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{3n+1}{4} & \text{if } \eta_1 = 0, \rho = 0 \\ n - \frac{3n+1}{4} & \text{if } \eta_1 = -1, \rho = 0 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = 0, \rho = 1 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_1 = 0$ and $\rho = 1$ or $\eta_1 = -1$ and $\rho = 1$, the minimum weight d of the code has the lower bound of Lemma 3.2, provided that $\text{ord}_n(q) = (n-1)/4$.

- 4) When $\frac{n+1-2u}{16} \equiv 1 \pmod{p}$ and $\frac{n-3+2u}{16} \not\equiv 0 \pmod{p}$, we distinguish between the two cases: p odd and $p = 2$.

If p is odd,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_2^{(4,n)}(x)} & \text{if } \eta_0 = 1, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_0^{(4,n)}(x)} & \text{if } \eta_0 = -1, \rho = 0 \\ x^n - 1 & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+3}{4} & \text{if } \eta_0 = 1, \rho = 0 \\ n - \frac{n+3}{4} & \text{if } \eta_0 = -1, \rho = 0 \\ n & \text{if } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_0 = 1$ and $\rho = 0$ or $\eta_0 = -1$ and $\rho = 0$, the minimum weight d of the code has the lower bound of Lemma 3.4, provided that $\text{ord}_n(q) = (n-1)/4$. If $p = 2$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \rho = 0 \\ x^n - 1 & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+1}{2} & \text{if } \rho = 0 \\ n & \text{if } \rho = 1. \end{cases}$$

In this subcase, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. Furthermore, the code is a quadratic residue code and hence $d \geq \sqrt{n}$ if $\rho = 0$ [23].

- 5) When $\frac{n+1-2u}{16} \not\equiv 0, 1 \pmod{p}$ and $\frac{n-3+2u}{16} \equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 1 \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+3}{4} & \text{if } \eta_1 = 0, \rho = 0 \\ n - \frac{n+3}{4} & \text{if } \eta_1 = -1, \rho = 0 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = 0, \rho = 1 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = -1, \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_1 = 0$ and $\rho = 0$ or $\eta_1 = -1$ and $\rho = 0$, the minimum weight d of the code has the lower bound of Lemma 3.4, provided that $\text{ord}_n(q) = (n-1)/4$. If $\eta_1 = 0$ and $\rho = 1$ or $\eta_1 = -1$ and $\rho = 1$, the minimum weight d of the code has the lower bound of Lemma 3.2, provided that $\text{ord}_n(q) = (n-1)/4$.

- 6) When $\frac{n+1-2u}{16} \not\equiv 0, 1 \pmod{p}$ and $\frac{n-3+2u}{16} \not\equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{x-1} & \text{if } \rho = 0 \\ x^n - 1 & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n-1 & \text{if } \rho = 0 \\ n & \text{if } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$, where $d = n$ if $\rho = 0$.

Proof: We prove the conclusions on the linear span and minimal polynomial of the sequence λ^∞ for Case 1 only. The conclusions of other cases can be similarly proved.

Since $n \equiv 1 \pmod{8}$, $-1 \in C_0^{(4,n)}$. By the definition of cyclotomic numbers, we have

$$\begin{aligned} \eta_\ell^2 &= \left(\sum_{i \in C_\ell^{(4,n)}} \eta^i \right)^2 \\ &= (\ell, \ell)_4 \eta_0 + (\ell+3, \ell+3)_4 \eta_1 + \\ &\quad (\ell+2, \ell+2)_4 \eta_2 + (\ell+1, \ell+1)_4 \eta_3 + \frac{n-1}{4}. \end{aligned}$$

It then follows from Table II and the cyclotomic numbers of order 4 for the case $n \equiv 1 \pmod{8}$ that

$$\begin{aligned} \eta_0^2 &= \frac{3n-1-2u}{16} - \frac{u+1}{2} \eta_0 + \frac{v}{2} \eta_1 - \frac{v}{2} \eta_3, \\ \eta_1^2 &= \frac{3n-1-2u}{16} - \frac{u+1}{2} \eta_1 + \frac{v}{2} \eta_2 - \frac{v}{2} \eta_0, \\ \eta_2^2 &= \frac{3n-1-2u}{16} - \frac{u+1}{2} \eta_2 + \frac{v}{2} \eta_3 - \frac{v}{2} \eta_1, \\ \eta_3^2 &= \frac{3n-1-2u}{16} - \frac{u+1}{2} \eta_3 + \frac{v}{2} \eta_0 - \frac{v}{2} \eta_2. \end{aligned}$$

Whence,

$$\begin{cases} \eta_0^2 + \eta_2^2 = \frac{3n-1-2u}{8} - \frac{u+1}{2}(\eta_0 + \eta_2), \\ \eta_1^2 + \eta_3^2 = \frac{3n-1-2u}{8} - \frac{u+1}{2}(\eta_1 + \eta_3). \end{cases} \quad (27)$$

Since $n \equiv 1 \pmod{8}$, $-1 \in C_0^{(4,n)}$. By the definition of cyclotomic numbers, we have

$$\begin{aligned} \eta_\ell \eta_{\ell+2} &= \sum_{i \in C_\ell^{(4,n)}} \sum_{j \in C_{\ell+2}^{(4,n)}} \eta^{i-j} \\ &= (\ell+2, \ell)_4 \eta_0 + (\ell+1, \ell+3)_4 \eta_1 + \\ &\quad (\ell, \ell+2)_4 \eta_2 + (\ell+3, \ell+1)_4 \eta_3. \end{aligned}$$

It then follows from the cyclotomic numbers of order 4 that

$$\begin{cases} \eta_0 \eta_2 = -\frac{n+1-2u}{16} + \frac{u-1}{4}(\eta_0 + \eta_2), \\ \eta_1 \eta_3 = -\frac{n+1-2u}{16} + \frac{u-1}{4}(\eta_1 + \eta_3). \end{cases} \quad (28)$$

Since $\frac{n-1}{4} \pmod{p} = 0$,

$$\Lambda(1) = \rho. \quad (29)$$

Recall that $\eta_0 + \eta_2 = 0$ and $\eta_1 + \eta_3 = -1$. In Case 1, by (27) and (28), we have

$$\eta_0 = \eta_2 = 0, \quad \eta_1(\eta_1 + 1) = \eta_3(\eta_3 + 1) = 0.$$

It then follows from (25) and (29) that

$$\gcd(\Lambda(x), x^n - 1) = \begin{cases} (x-1)\Omega_3^{(4,n)}(x) & \text{if } \eta_1 = 0 \text{ and } \rho = 0 \\ (x-1)\Omega_1^{(4,n)}(x) & \text{if } \eta_1 = -1 \text{ and } \rho = 0 \\ \Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x) & \text{if } \eta_1 = 0 \text{ and } \rho = 1 \\ \Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x) & \text{if } \eta_1 = -1 \text{ and } \rho = 1. \end{cases}$$

The desired conclusions on the linear span and the minimal polynomial of the sequence λ^∞ for Case 1 then follow from Lemma 2.1.

The desired conclusions on the dimension and the generator polynomial of the code \mathcal{C}_λ follow from the conclusions on the linear span and the minimal polynomial of the sequence λ^∞ and the definition of the code \mathcal{C}_λ . The conclusion on the minimum weight for each case follows from Lemmas (3.2) or (3.4), or the square-root bound on the minimum weight in quadratic residue codes, or the square-root bound on the minimum odd-like weight in duadic codes [19]. ■

Example 3.14: Let $(p, m, n) = (2, 1, 113)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-7)^2 + 4 \times 4^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 0 \text{ and } \frac{n-3+2u}{16} \bmod p = 0.$$

So this is Case 1. Let $\rho = 1$. Then \mathcal{C}_λ is a $[113, 84, 8]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^{29} + x^{27} + x^{26} + x^{22} + x^{21} + x^{18} + x^{16} + x^{13} + x^{11} + x^8 + x^7 + x^3 + x^2 + 1$$

The best binary linear code known of length 113 and dimension 84 has minimum weight 10.

Example 3.15: Let $(p, m, n) = (2, 1, 113)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-7)^2 + 4 \times 4^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 0 \text{ and } \frac{n-3+2u}{16} \bmod p = 0.$$

So this is Case 1. Let $\rho = 0$. Then \mathcal{C}_λ is a $[113, 29, 28]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned} & x^{84} + x^{82} + x^{81} + x^{80} + x^{76} + x^{75} + x^{74} + \\ & x^{73} + x^{72} + x^{70} + x^{68} + x^{66} + x^{65} + x^{64} + \\ & x^{63} + x^{62} + x^{60} + x^{59} + x^{58} + x^{57} + x^{56} + \\ & x^{55} + x^{53} + x^{47} + x^{46} + x^{43} + x^{42} + x^{41} + \\ & x^{38} + x^{37} + x^{31} + x^{29} + x^{28} + x^{27} + x^{26} + \\ & x^{25} + x^{24} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + \\ & x^{16} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + \\ & x^4 + x^3 + x^2 + 1. \end{aligned}$$

The best binary linear code known of length 113 and dimension 29 has minimum weight 32.

Example 3.16: Let $(p, m, n) = (2, 2, 41)$. Then $q = 4 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 1^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 0 \text{ and } \frac{n-3+2u}{16} \bmod p = 1.$$

So this is Case 2. Let $\rho = 0$. Then \mathcal{C}_λ is a $[41, 1, 41]$ cyclic code over $\text{GF}(q)$ with generator polynomial $(x^{41} - 1)/(x - 1)$.

Example 3.17: Let $(p, m, n) = (2, 2, 41)$. Then $q = 4 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 1^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 0 \text{ and } \frac{n-3+2u}{16} \bmod p = 1.$$

So this is Case 2. Let $\rho = 1$. Then \mathcal{C}_λ is a $[41, 20, 10]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^{21} + x^{19} + x^{18} + x^{16} + x^{15} + x^{14} + x^{12} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + 1.$$

Example 3.18: Let $(p, m, n) = (2, 1, 73)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 4^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 1 \text{ and } \frac{n-3+2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 0$. Then \mathcal{C}_λ is a $[73, 55, 6]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^{18} + x^{16} + x^{15} + x^{14} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^4 + x^3 + x^2 + 1.$$

This may be the first known binary cyclic code with parameters $[73, 55, 6]$. Earlier, only a linear code with the same parameters was known.

Example 3.19: Let $(p, m, n) = (2, 1, 89)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 4^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 1 \text{ and } \frac{n-3+2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 0$. Then \mathcal{C}_λ is a $[89, 67, 7]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^{22} + x^{19} + x^{17} + x^{15} + x^{12} + x^{11} + x^{10} + x^7 + x^5 + x^3 + 1.$$

The best linear code with length 89 and dimension 67 has minimum weight 8. This may be the first cyclic code known with parameters $[89, 67, 7]$.

Example 3.20: Let $(p, m, n) = (2, 1, 73)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 4^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 1 \text{ and } \frac{n-3+2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 1$. Then \mathcal{C}_λ is a $[73, 18, 24]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned} & x^{55} + x^{53} + x^{52} + x^{47} + x^{43} + x^{41} + x^{40} + \\ & x^{39} + x^{38} + x^{37} + x^{35} + x^{34} + x^{32} + x^{31} + \\ & x^{30} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{18} + \\ & x^{17} + x^{16} + x^{15} + x^{14} + x^{12} + x^8 + x^3 + x^2 + 1. \end{aligned}$$

This may be the first known binary cyclic code with parameters $[73, 18, 24]$. Earlier, only a linear code with the same parameters was known.

Example 3.21: Let $(p, m, n) = (2, 1, 89)$. Then $q = 2 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 4^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 1 \text{ and } \frac{n-3+2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 1$. Then \mathcal{C}_λ is a $[89, 22, 28]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned} & x^{67} + x^{64} + x^{62} + x^{61} + x^{60} + x^{58} + x^{53} + \\ & x^{52} + x^{51} + x^{50} + x^{48} + x^{47} + x^{45} + x^{44} + \\ & x^{41} + x^{39} + x^{36} + x^{31} + x^{28} + x^{26} + x^{23} + \\ & x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{14} + \\ & x^9 + x^7 + x^6 + x^5 + x^3 + 1. \end{aligned}$$

The best linear code with length 89 and dimension 22 has minimum weight 28. This may be the first cyclic code known with these parameters.

Example 3.22: Let $(p, m, n) = (2, 2, 17)$. Then $q = 4 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 1^2 + 4 \times 2^2$. Then

$$\frac{n+1-2u}{16} \bmod p = 1 \text{ and } \frac{n-3+2u}{16} \bmod p = 1.$$

So this is Case 4. Let $\rho = 0$. Then \mathcal{C}_λ is a $[17, 9, 5]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1.$$

The best linear code with length 17 and dimension 9 has minimum weight 7.

Remark 3.23: It was proved in [11] that $C_0^{(4,n)}$ is a $(n, (n-1)/4, (n-3)/16, (n-1)/2)$ almost difference set in $(\text{GF}(n), +)$ when $n = 5^2 + 4v^2$ or $n = (-3)^2 + 4v^2$. Examples 3.17, 3.20, and 3.21 show that the cyclic codes defined by such almost difference sets are very good.

Remark 3.24: It was proved in [12] that $C_0^{(4,n)} \cup \{0\}$ is a $(n, (n+3)/4, (n-5)/16, (n-1)/2)$ almost difference set in $(\text{GF}(n), +)$ when $n = 1^2 + 4v^2$ or $n = (-7)^2 + 4v^2$. Examples 3.15 and 3.22 indicate that the cyclic code defined by such almost difference sets are very good.

When $n \equiv 5 \pmod{8}$, the linear span and minimal polynomial of the sequence λ^∞ as well as the parameters of the code \mathcal{C}_λ are given in the following theorem.

Theorem 3.25: Let $\frac{n-1}{4} \equiv 0 \pmod{p}$ and $q \in C_0^{(4,n)}$, and let $n \equiv 5 \pmod{8}$. let λ^∞ be the sequence of period n over $\text{GF}(q)$ defined in (23). As before, $n = u^2 + 4v^2$ with $u \equiv 1 \pmod{4}$.

- 1) When $\frac{3n-1+2u}{16} \equiv 0 \pmod{p}$ and $\frac{3n+3-2u}{16} \equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = 0 \text{ and } \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = -1 \text{ and } \rho = 0 \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_1 = 0 \text{ and } \rho = 1 \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_1 = -1 \text{ and } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+3}{4} & \text{if } \eta_1 = 0 \text{ and } \rho = 0 \\ n - \frac{n+3}{4} & \text{if } \eta_1 = -1 \text{ and } \rho = 0 \\ n - \frac{3n-3}{4} & \text{if } \eta_1 = 0 \text{ and } \rho = 1 \\ n - \frac{3n-3}{4} & \text{if } \eta_1 = -1 \text{ and } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_1 = 0$ and $\rho = 0$ or $\eta_1 = -1$ and $\rho = 0$, the minimum weight d of the code has the lower bound of Lemma 3.4, provided that $\text{ord}_n(q) = (n-1)/4$.

- 2) When $\frac{3n-1+2u}{16} \equiv 0 \pmod{p}$ and $\frac{3n+3-2u}{16} \not\equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{x-1} & \text{if } \rho = 0 \\ \frac{x^n-1}{\Omega_0^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - 1 & \text{if } \rho = 0 \\ n - \frac{n-1}{2} & \text{if } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$, where

$$\begin{cases} d = n & \text{if } \rho = 0 \\ d \geq \sqrt{n} & \text{if } \rho = 1. \end{cases}$$

- 3) When $\frac{3n-1+2u}{16} \equiv p-1 \pmod{p}$ and $\frac{3n+3-2u}{16} \equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_0 = 1, \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)\Omega_2^{(4,n)}(x)} & \text{if } \eta_0 = 1, \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x)} & \text{if } \eta_0 = -1, \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x)} & \text{if } \eta_0 = \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 1 \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+1}{2} & \text{if } \eta_0 = 1, \eta_1 = 0, \rho = 0 \\ n - \frac{n+1}{2} & \text{if } \eta_0 = 1, \eta_1 = -1, \rho = 0 \\ n - \frac{n+1}{2} & \text{if } \eta_0 = -1, \eta_1 = 0, \rho = 0 \\ n - \frac{n+1}{2} & \text{if } \eta_0 = -1, \eta_1 = -1, \rho = 0 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = 0, \rho = 1 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = -1, \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_1 = 0$ and $\rho = 1$ or $\eta_1 = -1$ and $\rho = 1$, the minimum weight d of the code has the lower bound of Lemma 3.2, provided that $\text{ord}_n(q) = (n-1)/4$. In the rest four cases, the code is a duadic code and hence the minimum odd-like weight $d_{\text{odd}} \geq \sqrt{n}$.

- 4) When $\frac{3n-1+2u}{16} \equiv p-1 \pmod{p}$ and $\frac{3n+3-2u}{16} \not\equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_2^{(4,n)}(x)} & \text{if } \eta_0 = 1, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_0^{(4,n)}(x)} & \text{if } \eta_0 = -1, \rho = 0 \\ x^n - 1 & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+3}{4} & \text{if } \eta_0 = 1, \rho = 0 \\ n - \frac{n+3}{4} & \text{if } \eta_0 = -1, \rho = 0 \\ n & \text{if } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. In addition, if $\eta_0 = 1$ and $\rho = 0$ or $\eta_0 = -1$ and $\rho = 0$, the minimum weight d of the code has the lower bound of Lemma 3.4, provided that $\text{ord}_n(q) = (n-1)/4$.

- 5) When $\frac{3n-1+2u}{16} \not\equiv 0, p-1 \pmod{p}$ and $\frac{3n+3-2u}{16} \equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{(x-1)\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 0 \\ \frac{x^n-1}{(x-1)\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 0 \\ \frac{x^n-1}{\Omega_1^{(4,n)}(x)} & \text{if } \eta_1 = 0, \rho = 1 \\ \frac{x^n-1}{\Omega_3^{(4,n)}(x)} & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n - \frac{n+3}{4} & \text{if } \eta_1 = 0, \rho = 0 \\ n - \frac{n+3}{4} & \text{if } \eta_1 = -1, \rho = 0 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = 0, \rho = 1 \\ n - \frac{n-1}{4} & \text{if } \eta_1 = -1, \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$. Furthermore, if $\eta_1 = 0$ and $\rho = 0$ or $\eta_1 = -1$ and $\rho = 0$, the minimum weight d of the code has the lower bound of Lemma 3.4, provided that $\text{ord}_n(q) = (n-1)/4$. If $\eta_1 = 0$ and $\rho = 1$ or $\eta_1 = -1$ and $\rho = 1$, the minimum weight d of the code has the lower bound of Lemma 3.2, provided that $\text{ord}_n(q) = (n-1)/4$.

- 6) When $\frac{3n-1+2u}{16} \not\equiv 0, p-1 \pmod{p}$ and $\frac{3n+3-2u}{16} \not\equiv 0 \pmod{p}$,

$$m_\lambda(x) = \begin{cases} \frac{x^n-1}{x-1} & \text{if } \rho = 0 \\ x^n - 1 & \text{if } \rho = 1 \end{cases}$$

and

$$\mathbb{L}_\lambda = \begin{cases} n-1 & \text{if } \rho = 0 \\ n & \text{if } \rho = 1. \end{cases}$$

In this case, the cyclic code \mathcal{C}_λ over $\text{GF}(q)$ defined by the sequence λ^∞ has the generator polynomial $m_\lambda(x)$ and parameters $[n, n - \mathbb{L}_\lambda, d]$, where $d = n$ if $\rho = 0$.

Proof: We prove only the conclusion of Case 3. The conclusions of other cases can be similarly proved.

Since $n \equiv 5 \pmod{8}$, $-1 \in C_2^{(4,n)}$. Note that p must be odd, as $n \equiv 5 \pmod{8}$ and $\frac{n-1}{4} \pmod{p} = 0$. By the definition of cyclotomic numbers, we have

$$\begin{aligned} \eta_\ell^2 &= \left(\sum_{i \in C_\ell^{(4,n)}} \eta^i \right)^2 \\ &= \sum_{i \in C_\ell^{(4,n)}} \sum_{j \in C_{\ell+2}^{(4,n)}} \eta^{i-j} \\ &= (\ell+2, \ell)_4 \eta_0 + (\ell+1, \ell+3)_4 \eta_1 + \\ &\quad (\ell, \ell+2)_4 \eta_2 + (\ell+3, \ell+1)_4 \eta_3. \end{aligned}$$

It then follows from Table I and the cyclotomic numbers of order 4 for the case $n \equiv 1 \pmod{8}$ that

$$\begin{aligned} \eta_0^2 &= -\frac{n+1-6u}{16} + \frac{u-1}{2} \eta_0 + \frac{u-v}{2} \eta_1 - \frac{u+v}{2} \eta_3, \\ \eta_1^2 &= -\frac{n+1-6u}{16} + \frac{u-1}{2} \eta_1 + \frac{u-v}{2} \eta_2 - \frac{u+v}{2} \eta_0, \\ \eta_2^2 &= -\frac{n+1-6u}{16} + \frac{u-1}{2} \eta_2 + \frac{u-v}{2} \eta_3 - \frac{u+v}{2} \eta_1, \\ \eta_3^2 &= -\frac{n+1-6u}{16} + \frac{u-1}{2} \eta_3 + \frac{u-v}{2} \eta_0 - \frac{u+v}{2} \eta_2. \end{aligned}$$

Whence,

$$\begin{cases} \eta_0^2 + \eta_2^2 = -\frac{n+1+2u}{8} - \frac{u+1}{2}(\eta_0 + \eta_2), \\ \eta_1^2 + \eta_3^2 = -\frac{n+1+2u}{8} - \frac{u+1}{2}(\eta_1 + \eta_3). \end{cases} \quad (30)$$

Since $n \equiv 1 \pmod{8}$, $-1 \in C_2^{(4,n)}$. By the definition of cyclotomic numbers, we have

$$\begin{aligned} \eta_\ell \eta_{\ell+2} &= \sum_{i \in C_\ell^{(4,n)}} \sum_{j \in C_{\ell+2}^{(4,n)}} \eta^{i-j} \\ &= (\ell, \ell)_4 \eta_0 + (\ell+3, \ell+3)_4 \eta_1 + \\ &\quad (\ell+2, \ell+2)_4 \eta_2 + (\ell+1, \ell+1)_4 \eta_3 + \frac{n-1}{4}. \end{aligned}$$

It then follows from the cyclotomic numbers of order 4 that

$$\begin{cases} \eta_0\eta_2 = \frac{3n-1+2u}{16} + \frac{u-1}{4}(\eta_0 + \eta_2), \\ \eta_1\eta_3 = \frac{3n-1+2u}{16} + \frac{u-1}{4}(\eta_1 + \eta_3). \end{cases} \quad (31)$$

Since $\frac{n-1}{4} \bmod p = 0$,

$$\Lambda(1) = \rho. \quad (32)$$

Recall that $\eta_0 + \eta_2 = 0$ and $\eta_1 + \eta_3 = -1$. In Case 3, by (30) and (31), we have

$$\eta_0 = \eta_2 = 1, \quad \eta_1(\eta_1 + 1) = \eta_3(\eta_3 + 1) = 0.$$

It then follows from (25) and (32) that

$$\gcd(\Lambda(x), x^n - 1) = \begin{cases} (x-1)\Omega_3^{(4,n)}(x)\Omega_2^{(4,n)}(x) & \text{if } \eta_0 = 1, \eta_1 = 0, \rho = 0 \\ (x-1)\Omega_1^{(4,n)}(x)\Omega_2^{(4,n)}(x) & \text{if } \eta_0 = 1, \eta_1 = -1, \rho = 0 \\ (x-1)\Omega_3^{(4,n)}(x)\Omega_0^{(4,n)}(x) & \text{if } \eta_0 = -1, \eta_1 = 0, \rho = 0 \\ (x-1)\Omega_1^{(4,n)}(x)\Omega_0^{(4,n)}(x) & \text{if } \eta_0 = \eta_1 = -1, \rho = 0 \\ \Omega_1^{(4,n)}(x) & \text{if } \eta_1 = 0, \rho = 1 \\ \Omega_3^{(4,n)}(x) & \text{if } \eta_1 = -1, \rho = 1 \end{cases}$$

The desired conclusions on the linear span and the minimal polynomial of the sequence λ^∞ for Case 3 then follow from Lemma 2.1.

The desired conclusions on the dimension and the generator polynomial of the code \mathcal{C}_λ follow from the conclusions on the linear span and the minimal polynomial of the sequence λ^∞ and the definition of the code \mathcal{C}_λ . The conclusion on the minimum weight for each case follows from Lemmas (3.2) or (3.4), or the square-root bound on the minimum weight in quadratic residue codes, or the square-root bound on the minimum odd-like weight in duadic codes [19]. ■

Example 3.26: Let $(p, m, n) = (3, 2, 61)$. Then $q = 9 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 3^2$. Then

$$\frac{3n-1+2u}{16} \bmod p = 0 \text{ and } \frac{3n+3-2u}{16} \bmod p = 2.$$

So this is Case 2. Let $\rho = 1$. Then \mathcal{C}_λ is a $[61, 30, 12]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^{31} + x^{29} + 2x^{28} + 2x^{27} + 2x^{26} + x^{25} + 2x^{22} + x^{19} + \\ 2x^{16} + x^{15} + 2x^{12} + x^9 + 2x^6 + x^5 + x^4 + x^3 + 2x^2 + 2.$$

The best linear code over $\text{GF}(q)$ with length 61 and dimension 30 has minimum weight 20.

Example 3.27: Let $(p, m, n) = (3, 1, 13)$. Then $q = 3 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 1^2$. Then

$$\frac{3n-1+2u}{16} \bmod p = 2 \text{ and } \frac{3n+3-2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 0$. Then \mathcal{C}_λ is a $[13, 7, 4]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1.$$

The optimal linear code over $\text{GF}(q)$ with length 13 and dimension 7 has minimum weight 5. The code of this example is almost optimal and cyclic.

Example 3.28: Let $(p, m, n) = (3, 1, 13)$. Then $q = 3 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 1^2$. Then

$$\frac{3n-1+2u}{16} \bmod p = 2 \text{ and } \frac{3n+3-2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 1$. Then \mathcal{C}_λ is a $[13, 3, 9]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$x^{10} + x^8 + x^7 + x^6 + 2x^5 + 2x^4 + x^2 + 2x + 1.$$

The known optimal linear code over $\text{GF}(q)$ with length 13 and dimension 3 has minimum weight 9. The code of this example is both optimal and cyclic.

Example 3.29: Let $(p, m, n) = (3, 1, 109)$. Then $q = 3 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = (-3)^2 + 4 \times 5^2$. Then

$$\frac{3n - 1 + 2u}{16} \bmod p = 2 \text{ and } \frac{3n + 3 - 2u}{16} \bmod p = 0.$$

So this is Case 3. Let $\rho = 1$. Then \mathcal{C}_λ is a $[109, 27, 42]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned} & x^{82} + 2x^{80} + 2x^{79} + x^{78} + x^{77} + 2x^{76} + 2x^{75} + x^{74} + \\ & x^{73} + 2x^{72} + 2x^{70} + 2x^{69} + 2x^{66} + 2x^{65} + 2x^{64} + 2x^{63} + \\ & 2x^{62} + 2x^{58} + x^{57} + x^{56} + 2x^{55} + x^{53} + 2x^{52} + 2x^{51} + \\ & 2x^{50} + x^{49} + 2x^{48} + 2x^{46} + 2x^{45} + x^{44} + 2x^{42} + x^{40} + \\ & 2x^{39} + 2x^{38} + 2x^{35} + 2x^{32} + x^{31} + x^{29} + 2x^{28} + 2x^{27} + \\ & x^{26} + x^{25} + x^{24} + x^{22} + x^{21} + x^{20} + 2x^{16} + 2x^{15} + \\ & 2x^{14} + x^{12} + x^{11} + 2x^8 + x^7 + 2x^5 + x^3 + 2x + 1. \end{aligned}$$

This has the same parameters as the best known code with length 109 and dimension 27 which is also cyclic.

Example 3.30: Let $(p, m, n) = (7, 1, 29)$. Then $q = 7 \in C_0^{(4,n)}$ and $n = u^2 + 4v^2 = 5^2 + 4 \times 1^2$. Then

$$\frac{3n - 1 + 2u}{16} \bmod p = 6 \text{ and } \frac{3n + 3 - 2u}{16} \bmod p = 5.$$

So this is Case 4. Let $\rho = 0$. Then \mathcal{C}_λ is a $[29, 8, 15]$ cyclic code over $\text{GF}(q)$ with generator polynomial

$$\begin{aligned} & x^{21} + 3x^{19} + 2x^{18} + 5x^{17} + 5x^{16} + 6x^{15} + 5x^{14} + \\ & 4x^{13} + 4x^{12} + x^{11} + 3x^{10} + x^9 + 4x^8 + 5x^7 + \\ & x^6 + x^5 + 6x^4 + 3x^3 + 4x^2 + 5x + 6. \end{aligned}$$

The known optimal linear code over $\text{GF}(q)$ with length 29 and dimension 8 has minimum weight 17.

Remark 3.31: It was proved in [11] that $C_0^{(4,n)}$ is an $(n, (n-1)/4, (n-3)/16, (n-1)/2)$ almost difference set in $(\text{GF}(n), +)$ when $n = (-3)^2 + 4v^2$ or $n = 5^2 + 4v^2$. Examples 3.26, 3.28 and 3.29 show that the cyclic code defined by such almost difference sets are very good.

Remark 3.32: It is known that $C_0^{(4,n)} \cup \{0\}$ is an $(n, (n-1)/4, (n+3)/16)$ difference set in $(\text{GF}(n), +)$ when $n = (-3)^2 + 4v^2$ and v is odd. Examples 3.15 may indicate that the cyclic code defined by such difference sets are very good.

Open Problem 3.33: Determine the parameters of the code \mathcal{C}_λ defined by the sequence λ^∞ of (23) for the case that $\frac{n-1}{4} \not\equiv 0 \pmod{p}$.

IV. CONCLUDING REMARKS

Perfect difference sets were used to construct cyclic codes in [27]. The idea of constructing cyclic codes with special types of sequences employed in this paper could be viewed as an extension of this idea.

There are several bounds on cyclic codes [2], [5], [7], [6], [18], [22]. It may not be easy to employ them to get tight bounds on the minimum weight of the cyclic codes presented in this paper. The actual minimum weight of these codes depends on the distribution of biquadratic residues modulo n , which looks to be a hard problem. However, some of the codes obtained in this paper are quadratic residue codes and duadic codes, which have a square-root bound on the minimum weight and the minimum odd-like

weight respectively. In addition, we developed lower bounds on the minimum weight d of some cyclic codes under certain conditions. It would be nice if tight lower bounds on the minimum weight could be developed for the remaining cases.

As a subclass of linear codes, cyclic codes usually have a smaller minimum weight compared with linear codes of the same length and dimension. However, some cyclic codes are optimal in the sense that they meet bounds defined for all linear codes. For example, the cyclic code of Example 3.9 is optimal. It is interesting to note that many of the example codes presented in this paper are the best possible cyclic codes and some are as good as the best linear codes with the same length and dimension. For example, the binary cyclic code of Example 3.21 has parameters $[89, 22, 28]$, which has the same parameters as the record binary linear code. These examples demonstrate that the cyclic codes defined by the cyclotomic sequences of order four are very good in general, but could be bad sometimes.

The p -rank of the almost difference sets and difference sets is defined to be the linear span of the sequences over $\text{GF}(p)$ defined by the almost difference sets and difference sets. The p -ranks of the almost difference sets and difference sets can be used to distinguish them from other almost difference sets and difference sets. This is the contribution of this paper to combinatorics. The contribution of this paper to the theory of sequences and cryptography is the computation of the linear span of these cyclotomic sequences of order four.

REFERENCES

- [1] K. T. Arasu, C. Ding, T. Helleseeth, P. V. Kumar, H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Information Theory*, vol. 47, pp. 2834–2943, 2001.
- [2] D. Augot and F. Levy-dit Vehel, "Bounds on the minimum distance of the duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 4, pp. 1257–1260, 1996.
- [3] B.C. Berndt, R.J. Evans and K. S. Williams, *Gauss and Jacobi sums*, New York: J.Wiley and Sons Company, 1997.
- [4] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd Edition, Cambridge University Press, 1999.
- [5] E. Betti and M. Sala, "A new bound for the minimum distance of a cyclic code from its defining set," *IEEE Trans. Inform. Theory*, vol. 52, no. 8, pp. 3700–3706, 2006.
- [6] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, 1960.
- [7] N. Boston, "Bounding minimum distances of cyclic codes using algebraic geometry," *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 385–394, 2000.
- [8] P. Charpin, Open problems on cyclic codes, in *Handbook of Coding Theory*, Part 1: Algebraic Coding, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 11.
- [9] R. T. Chien, "Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes," *IEEE Trans. Inform. Theory*, vol. 10, pp. 357–363, October 1964.
- [10] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 21, no. 5, pp. 575–576, Sept. 1975.
- [11] C. Ding, *Cryptographic Counter Generators*, TUCS Series in Dissertation 4, Turku Centre for Computer Science, 1997, ISBN 951-650-929-0.
- [12] C. Ding, T. Helleseeth and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2606–2612, Nov. 1999.
- [13] C. Ding, K. Y. Lam and C. Xing, "Enumeration and construction of all duadic codes of length p^m ," *Fundamenta Informaticae*, vol. 38, no. 1, pp. 149–161, 1999.
- [14] C. Ding and V. Pless, "Cyclotomy and duadic codes of prime lengths," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, 453–466, 1999.
- [15] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," preprint, 2011.
- [16] M. van Eupen and J. H. van Lint, "On the minimum distance of ternary cyclic codes," *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 409–416, March 1993.
- [17] G. D. Forney, "On decoding BCH codes," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 549–557, October 1965.
- [18] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, pp. 489–498, 1972.
- [19] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [20] J. S. Leon, J. M. Masley, and V. Pless, "Duadic codes," *IEEE Trans. Inform. Theory*, vol. 30, pp. 709–714, 1984.
- [21] L. Lidl, and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [22] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 23–40, Jan. 1986.
- [23] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, Vol. 16, North-Holland, Amsterdam, 1977.
- [24] V. Pless, J. M. Masley, and J. S. Leon, "On weights in duadic codes," *J. Comb. Theory*, vol. A 44, pp. 6–21, 1987.
- [25] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," Air Force Cambridge Research Center-TN-58-156, Cambridge, Mass., April 1958.

- [26] T. Storer, *Cyclotomy and Difference Sets*, Chicago: Markham, 1967.
- [27] E. J. Weldon, Jr., Difference-set cyclic codes, *Bell Syst. Tech. J.*, vol. 45, pp. 1045-1055, Sept. 1966.